DEPARTMENT OF THE NAVY
HEADQUARTERS
NAVAL SECURITY AND INVESTIGATIVE COMMAND
WASHINGTON, D.C. 20388

IN REPLY REFER TO

5500
NSIC-212B/443
27 AUG 1987

From: Commander, Naval Security and Investigative Command
To: [redacted] Chairman, Personnel Security Committee STAT

Subj: SURVEY OF FOREIGN TRAVEL REPORTING REQUIREMENTS

Ref: (a) Memo for Members, IG/CM(P), Subj: Survey of Foreign Travel Reporting Requirements

Encl: (1) Portions of OPNAVINST 5510.1H pertaining to foreign travel reporting requirements

1. In response to reference (a), the following is submitted, keyed to numbered questions of the Foreign Travel Reporting Survey:

Question 1: All foreign travel must be reported by all accessed employees in advance of performing such travel. This is a mandatory requirement.

Question 2: Not applicable. No exceptions apply.

Question 3: DOD 5200.2-R, Department of Defense Personnel Security Program and OPNAVINST 5510.1H, Department of the Navy (DON) Information and Personnel Security Program provide the regulatory basis for this reporting requirement.

Question 4: Employees are advised of their obligation to report foreign travel during their initial orientation briefing, when granted access, and during annual refresher briefings.

Question 5: Adjudication policy could be modified to include willful failure to report foreign travel as a disqualifying factor for possession of a security clearance.

Question 6: Employees overseas may be treated differently based on the particular local threat assessment. Briefings are tailored by local commands to reflect any such unusual threats.

Question 7: The DON utilizes no particular format as a vehicle for reporting. Reports are usually made in person by the prospective traveller to the local security office.

Question 8: Reports usually include the route and mode of travel, destination, length of stay, identity of fellow travellers (when accompanying the traveller) and identity of tour operator (if a tour operator is used).

Question 9: This report is received and evaluated by the local security office. No approval is required for travel to be performed to non-communist countries or for travel to communist

controlled countries for persons that do not have access to Sensitive Compartmented Information (SCI). Approval for travel to or through communist controlled countries is only required when the prospective traveller has access to SCI. Approval is then determined by the Special Security Officer.

Question 10: Only employees travelling to or through communist controlled countries are given a defensive briefing. These briefings may be conducted by the Naval Investigative Service (NIS) or the local security office. As a minimum, the content of the briefing is coordinated with the local NIS office to ensure that a current threat assessment is included, as well as current advise concerning: risk of capture; personal protection; harassments and provocations; appropriate manner of personal conduct; counterterrorism; and general travel advice.

Question 11: Foreign travel reports are maintained by the security office. When debriefings upon return from communist country related travel reveal unusual occurrences that could have security implications, an additional report may be made and maintained by the NIS. NIS files are available to other agencies conducting a National Agency Check (NAC). Reports maintained by the local security office would not be reported to an agency conducting a NAC (unless the NAC had been requested by the local security office holding the report). Reports are maintained by local security offices as long as the subject of the report is assigned/employed at that activity. NIS reports may be kept on file for up to 15 years, or perhaps longer, depending on the exact nature of the report.

Question 12: Locally held reports of foreign travel are reviewed as part of a local files check conducted prior to initiating a periodic reinvestigation. When considering the continued eligibility of a clearance holder following a security incident, the report may be considered, should it be determined that the report of foreign travel may have a bearing on the subject's continued eligibility.

Question 13: Agree with all elements identified in subparagraphs a through h.

ROBERT C. ALLEN
Director
Information and Personnel
Security Policy

ENCLOSURE 1

EXCERPTS FROM
OPNAVINST 5510.1H

2-8 DUTIES OF THE SECURITY MANAGER

1. The security manager is the principal advisor on information and personnel security in the command and is responsible for the management of the program. That doesn't necessarily mean that he/she personally handles all of the security duties described below. Many commands are organized to assign like duties to the same person and the personnel officer may be handling personnel security; the administrative officer may have classified material control; the training officer may be responsible for security education sessions, etc. Those assigned security duties may even be senior to the security manager. But, the security manager has to know what is going on in these areas, to ensure that the various pieces of the security program fit together and nothing falls through the cracks, that those in the command who have security duties are kept abreast of changes in policies and procedures, and to provide assistance in solving security problems. The job may involve direct supervision, oversight, coordination, or a combination thereof. However the command is organized, the security manager is the key in developing and administering the command's Information and Personnel Security Program.

2. The duties which follow, with the possible exception of those requiring preparation of classification guides and dealings with industrial contractors or foreign governments, apply to every security manager. In formulating the program for a command, the following list will help to identify the elements which apply to all commands, bearing in mind that many command security problems stem from a failure to appreciate the scope of the command's, and the security manager's responsibilities.

3. For effective management of the program, the security manager:

a. Serves as the commanding officer's advisor and direct representative in matters pertaining to the security of classified information and personnel security.

b. Develops written command information and personnel security procedures, including an emergency plan. Integrates emergency destruction bills with the emergency plan where required.

c. Formulates and coordinates the security education program in the command.

d. Ensures that threats to security, compromises and other security violations are reported, recorded and, when necessary, investigated vigorously. Ensures incidents falling under the investigative jurisdiction of the Naval Investigative Service are immediately referred to the nearest NIS office (see appendix D).

e. Administers the command's program for classification, declassification and downgrading of classified information.

f. Coordinates the preparation of classification guides in the command.

g. Maintains liaison with the command's public affairs officer to ensure that proposed press releases which could contain classified information are referred for security review.

h. Ensures compliance with accounting and control requirements for classi-fied material, including receipt, distribution, inventory, reproduction and disposition.

i. Formulates and coordinates physical security measures for protection of classified material.

j. Ensures that any electrical or electronic processing equipment meets control of compromising emanations (TEMPEST) requirements.

k. Ensures security control of classified visits to and from the command.

l. Ensures protection of classified information during unclassified visits to the command.

m. Prepares recommendations for release of classified information to foreign governments.

n. Ensures compliance with the Industrial Security Program for classified contracts with DOD contractors.

o. Ensures that all personnel who are to handle classified information or to be assigned to sensitive duties are appropriately cleared and that requests for personnel security investigations are properly prepared, submitted and monitored.

p. Ensures that access to classified information is limited to those with the need to know.

q. Ensures that personnel security investigations, clearances and access are recorded.

r. Coordinates the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

s. Maintains liaison with the command Special Security Officer concerning investigations, access to sensitive compartmented information (SCI), continuous evaluation of eligibility, and changes to information and personnel security policies and procedures.

t. Maintains records of personal foreign travel reported by assigned personnel. These records should identify, whenever possible, the travellers route and mode of travel, destination, length of stay, identity of fellow travellers (when accompanying the traveller) and identity of tour operator (if a tour operator is used).

3-4 SCOPE

1. Some security education must be provided to all personnel, whether they have access to classified information or not. More extensive education must be provided for those who do have access. The education effort must be tailored to meet the needs of the command, as well as those of different groups within the command.

2. In formulating a command security education program, the security manager must provide for the minimum briefing requirements but guard against allowing the program to evolve into a perfunctory compliance with the formal requirements without achieving the real goals. For instance, if the same lecture is given or the same film is shown every year, it could be said that the refresher briefing had been satisfied but it could not be said that security awareness was enhanced. Guidelines for developing an effective security education program are outlined in exhibit 3A.

3. Design the overall program to:

a. Advise personnel of the adverse effects to the national security which could result from unauthorized disclosure and of their personal, moral and legal responsibility to protect classified information within their knowledge, possession or control;

b. Advise personnel of their responsibility to adhere to the standards of conduct required of persons holding positions of trust and to avoid personal behavior which could render them ineligible for access or assignment to sensitive duties;

c. Advise personnel of their obligation to notify their supervisor or command security manager when they become aware of information with potentially serious security significance regarding someone with access to classified information or assigned to sensitive duties;

d. Advise supervisors of the requirement for continuous evaluation of personnel for eligibility for access to classified information or assignment to sensitive duties;

e. Familiarize personnel with the principles, criteria and procedures for the classification, downgrading, declassification, marking, control and accountability, storage, destruction, and transmission of classified infor-mation and material and alert them to the strict prohibitions against improper use and abuse of the classification system;

f. Familiarize personnel with procedures for challenging classification decisions believed to be improper;

g. Familiarize personnel with the security requirements for their particular assignment;

h. Instruct personnel that individuals having knowledge, possession or control of classified information must determine, before disseminating the information, that the prospective recipient has been authorized access by

competent authority, needs the information to perform his/her official duties, and can properly protect (store) the information;

i. Advise personnel of the strict prohibition against discussing classi-fied information over an unsecure telephone or in any other manner that permits interception by unauthorized persons;

j. Inform personnel of the techniques employed by foreign intelligence activities in attempting to obtain classified information;

k. Advise personnel of the penalties for engaging in espionage activities;

l. Advise personnel that they are required to report, in accordance with chapter 5:

(1) Any contact, intentional or unintentional, with a citizen, official, office, establishment or entity of a designated country (exhibit 5A);

(2) Information concerning any international or domestic terrorist organization, sabotage, or subversive activity that could reasonably pose or have a potential to pose a direct threat to DOD or other U.S. facilities activities, personnel or resources;

(3) A request by anyone, regardless of nationality, for illegal or unauthorized access to classified or controlled defense information; or

(4) Any contact with an individual, regardless of nationality, under circumstances which suggest the DON member may be the target of an attempted exploitation by the intelligence services of another country, such as:

(a) Attempts to cultivate friendship to the extent of placing one under obligation that could not normally be reciprocated;

(b) Offers of money payments or bribery to obtain information of actual or potential intelligence value; or

(c) Attempts to coerce by blackmail, threats against or promises of assistance to relatives living under foreign control.

m. Advise personnel of their obligation to notify their supervisor or command security manager before contacting or visiting any establishment of a designated country, including those located in the United States and friendly countries, and that subsequent to any visit or contact, the reporting require-ment of paragraph 1 (1) above applies; and

n. Advise personnel with access to classified information that all personal foreign travel must be reported in advance to the command security manager.

3-7 ORIENTATION

1. Each person who will have access to classified information will be given an orientation briefing as soon as possible after reporting aboard or being assigned to duties involving classified access.

2. The timing and format for orientation will vary, depending on the size of the command. At large commands with a high turnover rate, briefings may be scheduled on a regular basis. At smaller commands, with irregular changes of personnel, individual instruction may be necessary. However, orientation in a command that is formatted, having an individual certify that he/she has "read and understands" provisions of this regulation is not adequate orientation. The command security organization will be described and the security manager, identified by name. The new arrival must be given sufficient information to realize that he/she is now an essential link in the security structure of the command and is expected to function as a responsible member of that structure. The security manager must ensure that the new member is told about any special security precautions for the command. For instance, in a command with foreign nationals as students or in personnel exchange programs, the new member should be alerted to the restrictions on access by foreign nationals; or, if the command has a coded badge system, the significance of the codes should be explained.

3. Individual security responsibilities should be reviewed: the prohibition against discussing classified information in a nonsecure area, over a telephone, or in any other way that would allow access by an unauthorized person; the requirements of paragraph 3-4 of the obligation to report information which could reflect on the trustworthiness of an individual who has access to classified information.

4. The security orientation should be tailored to the command and to the individual receiving it. More emphasis on security procedures will be needed when the new member has not had previous experience with handling classified information.

5. All personnel will be advised during the orientation of the requirement to report any proposed personal foreign travel prior to commencing such travel to the command security manager.

3-9 REFRESHER BRIEFINGS

1. Once a year, all personnel who have access to classified information are to receive a refresher briefing. The purpose of the refresher briefing is to enhance security awareness. It should not be a rehash of the basics, talking down to those who have had access over a period of time, or a tired repeat of the same program year after year.

2. The annual refresher briefing may be addressed to the entire command on general security matters, changes in policies or procedures, or those topics required by paragraph 3-3 not being covered otherwise. It will include repetition of the reporting requirements of paragraph 3-4.

3. The refresher briefing does not have to cover the whole subject of security. As it is unlikely that it will be possible to schedule everyone in the command at the same time, the refresher briefing will probably be more effective if it is tailored for a particular group. For example, the briefing might include some updating on policies and procedures, plus required counter-intelligence reminders, but concentrate on preparation of classified material for clerical personnel or on procedures for classifying and marking material for those who draft classified documents. A review of the

requirements governing handcarrying classified material would be appropriate for those who are most likely to travel on command business or a review of clearance criteria and adjudicative policy would be appropriate for supervisors of cleared personnel.

4. Once every two years, those who have access to Secret or above must be given a counterespionage briefing by a Naval Investigative Service agent. The security manager is responsible for arranging for the briefing with the local NIS office (see appendix D).

3-10 SPECIAL BRIEFINGS

1. Certain types of special briefings are required, to be coordinated by the security manager. These include:

a. Foreign Travel Briefing

(1) Any individual who has had access to classified information who plans to travel to or through a communist controlled country or to attend a meeting, in the United States or elsewhere, in which representatives of communist controlled countries are expected to participate (see exhibit 5A), must be given a defensive briefing. Cruises on Soviet ships, which have become available recently, also require this precautionary briefing. It is recommended that the briefing be coordinated with the Naval Investigative Service.

(2) Audiovisual material for a formal Foreign Travel Briefing is stock-ed at servicing Naval Investigative Service offices (appendix D). Ensure that personnel know that this is a required briefing and that they are responsible for advising the security manager when a situation requiring a "foreign travel" briefing arises.

(3) When the individual returns, he/she should be debriefed to provide the opportunity to report any incident - no matter how insignificant it might have seemed - that could have security implications. A record should be kept of those given the briefing, for follow-up. Check with the Naval Investigative Service office, at the time the audiovisual material is requested, to see if NIS will accomplish the debriefing.

(4) Those who frequently travel, attend meetings or host meetings for foreign visitors need not be briefed at each occasion. Once every six months will suffice.

(5) The foreign travel briefing is only required for those who have had access to classified information but it may be given to dependents, or others without access, if they ask.

5-6 FOREIGN TRAVEL

1. All personnel possessing a security clearance are required to report to their security office all personal foreign travel in advance of the travel being performed. Personnel will be advised of this requirement to report such travel during the orientation briefing and annual refreshers briefings conducted in accordance with paragraphs 3-7 and 3-9.

2. When travel patterns (i.e., numerous expensive trips abroad or very frequent travel), or the failure to report such travel, indicate the need for investigation, the matter will be referred to the nearest NIS office for action and to the Commander, Naval Security and Investigative Command for information.

ENCLOSURE 1

EXCERPTS FROM
OPNAVINST 5510.1H

2-8 DUTIES OF THE SECURITY MANAGER

1. The security manager is the principal advisor on information and personnel security in the command and is responsible for the management of the program. That doesn't necessarily mean that he/she personally handles all of the security duties described below. Many commands are organized to assign like duties to the same person and the personnel officer may be handling personnel security; the administrative officer may have classified material control; the training officer may be responsible for security education sessions, etc. Those assigned security duties may even be senior to the security manager. But, the security manager has to know what is going on in these areas, to ensure that the various pieces of the security program fit together and nothing falls through the cracks, that those in the command who have security duties are kept abreast of changes in policies and procedures, and to provide assistance in solving security problems. The job may involve direct supervision, oversight, coordination, or a combination thereof. However the command is organized, the security manager is the key in developing and administering the command's Information and Personnel Security Program.

2. The duties which follow, with the possible exception of those requiring preparation of classification guides and dealings with industrial contractors or foreign governments, apply to every security manager. In formulating the program for a command, the following list will help to identify the elements which apply to all commands, bearing in mind that many command security problems stem from a failure to appreciate the scope of the command's, and the security manager's responsibilities.

3. For effective management of the program, the security manager:

a. Serves as the commanding officer's advisor and direct representative in matters pertaining to the security of classified information and personnel security.

b. Develops written command information and personnel security procedures, including an emergency plan. Integrates emergency destruction bills with the emergency plan where required.

c. Formulates and coordinates the security education program in the command.

d. Ensures that threats to security, compromises and other security violations are reported, recorded and, when necessary, investigated vigorously. Ensures incidents falling under the investigative jurisdiction of the Naval Investigative Service are immediately referred to the nearest NIS office (see appendix D).

e. Administers the command's program for classification, declassification and downgrading of classified information.

f. Coordinates the preparation of classification guides in the command.

g. Maintains liaison with the command's public affairs officer to ensure that proposed press releases which could contain classified information are referred for security review.

h. Ensures compliance with accounting and control requirements for classi-fied material, including receipt, distribution, inventory, reproduction and disposition.

i. Formulates and coordinates physical security measures for protection of classified material.

j. Ensures that any electrical or electronic processing equipment meets control of compromising emanations (TEMPEST) requirements.

k. Ensures security control of classified visits to and from the command.

l. Ensures protection of classified information during unclassified visits to the command.

m. Prepares recommendations for release of classified information to foreign governments.

n. Ensures compliance with the Industrial Security Program for classified contracts with DOD contractors.

o. Ensures that all personnel who are to handle classified information or to be assigned to sensitive duties are appropriately cleared and that requests for personnel security investigations are properly prepared, submitted and monitored.

p. Ensures that access to classified information is limited to those with the need to know.

q. Ensures that personnel security investigations, clearances and access are recorded.

r. Coordinates the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

s. Maintains liaison with the command Special Security Officer concerning investigations, access to sensitive compartmented information (SCI), continuous evaluation of eligibility, and changes to information and personnel security policies and procedures.

t. Maintains records of personal foreign travel reported by assigned personnel. These records should identify, whenever possible, the travellers route and mode of travel, destination, length of stay, identity of fellow travellers (when accompanying the traveller) and identity of tour operator (if a tour operator is used).

3-4 SCOPE

1. Some security education must be provided to all personnel, whether they have access to classified information or not. More extensive education must be provided for those who do have access. The education effort must be tailored to meet the needs of the command, as well as those of different groups within the command.

2. In formulating a command security education program, the security manager must provide for the minimum briefing requirements but guard against allowing the program to evolve into a perfunctory compliance with the formal requirements without achieving the real goals. For instance, if the same lecture is given or the same film is shown every year, it could be said that the refresher briefing had been satisfied but it could not be said that security awareness was enhanced. Guidelines for developing an effective security education program are outlined in exhibit 3A.

3. Design the overall program to:

a. Advise personnel of the adverse effects to the national security which could result from unauthorized disclosure and of their personal, moral and legal responsibility to protect classified information within their knowledge, possession or control;

b. Advise personnel of their responsibility to adhere to the standards of conduct required of persons holding positions of trust and to avoid personal behavior which could render them ineligible for access or assignment to sensitive duties;

c. Advise personnel of their obligation to notify their supervisor or command security manager when they become aware of information with potentially serious security significance regarding someone with access to classified information or assigned to sensitive duties;

d. Advise supervisors of the requirement for continuous evaluation of personnel for eligibility for access to classified information or assignment to sensitive duties;

e. Familiarize personnel with the principles, criteria and procedures for the classification, downgrading, declassification, marking, control and accountability, storage, destruction, and transmission of classified infor-mation and material and alert them to the strict prohibitions against improper use and abuse of the classification system;

f. Familiarize personnel with procedures for challenging classification decisions believed to be improper;

g. Familiarize personnel with the security requirements for their particular assignment;

h. Instruct personnel that individuals having knowledge, possession or control of classified information must determine, before disseminating the information, that the prospective recipient has been authorized access by

competent authority, needs the information to perform his/her official duties, and can properly protect (store) the information;

i. Advise personnel of the strict prohibition against discussing classi-fied information over an unsecure telephone or in any other manner that permits interception by unauthorized persons;

j. Inform personnel of the techniques employed by foreign intelligence activities in attempting to obtain classified information;

k. Advise personnel of the penalties for engaging in espionage activities;

l. Advise personnel that they are required to report, in accordance with chapter 5:

(1) Any contact, intentional or unintentional, with a citizen, official, office, establishment or entity of a designated country (exhibit 5A);

(2) Information concerning any international or domestic terrorist organization, sabotage, or subversive activity that could reasonably pose or have a potential to pose a direct threat to DOD or other U.S. facilities activities, personnel or resources;

(3) A request by anyone, regardless of nationality, for illegal or unauthorized access to classified or controlled defense information; or

(4) Any contact with an individual, regardless of nationality, under circumstances which suggest the DON member may be the target of an attempted exploitation by the intelligence services of another country, such as:

(a) Attempts to cultivate friendship to the extent of placing one under obligation that could not normally be reciprocated;

(b) Offers of money payments or bribery to obtain information of actual or potential intelligence value; or

(c) Attempts to coerce by blackmail, threats against or promises of assistance to relatives living under foreign control.

m. Advise personnel of their obligation to notify their supervisor or command security manager before contacting or visiting any establishment of a designated country, including those located in the United States and friendly countries, and that subsequent to any visit or contact, the reporting requirement of paragraph 1 (1) above applies; and

n. Advise personnel with access to classified information that all personal foreign travel must be reported in advance to the command security manager.

3-7 ORIENTATION

1. Each person who will have access to classified information will be given an orientation briefing as soon as possible after reporting aboard or being assigned to duties involving classified access.

2. The timing and format for orientation will vary, depending on the size of the command. At large commands with a high turnover rate, briefings may be scheduled on a regular basis. At smaller commands, with irregular changes of personnel, individual instruction may be necessary. However, orientation in a command that is formatted, having an individual certify that he/she has "read and understands" provisions of this regulation is not adequate orientation. The command security organization will be described and the security manager, identified by name. The new arrival must be given sufficient information to realize that he/she is now an essential link in the security structure of the command and is expected to function as a responsible member of that structure. The security manager must ensure that the new member is told about any special security precautions for the command. For instance, in a command with foreign nationals as students or in personnel exchange programs, the new member should be alerted to the restrictions on access by foreign nationals; or, if the command has a coded badge system, the significance of the codes should be explained.

3. Individual security responsibilities should be reviewed: the prohibition against discussing classified information in a nonsecure area, over a telephone, or in any other way that would allow access by an unauthorized person; the requirements of paragraph 3-4 of the obligation to report infor-mation which could reflect on the trustworthiness of an individual who has access to classified information.

4. The security orientation should be tailored to the command and to the individual receiving it. More emphasis on security procedures will be needed when the new member has not had previous experience with handling classified information.

5. All personnel will be advised during the orientation of the requirement to report any proposed personal foreign travel prior to commencing such travel to the command security manager.

3-9 REFRESHER BRIEFINGS

1. Once a year, all personnel who have access to classified information are to receive a refresher briefing. The purpose of the refresher briefing is to enhance security awareness. It should not be a rehash of the basics, talking down to those who have had access over a period of time, or a tired repeat of the same program year after year.

2. The annual refresher briefing may be addressed to the entire command on general security matters, changes in policies or procedures, or those topics required by paragraph 3-3 not being covered otherwise. It will include repetition of the reporting requirements of paragraph 3-4.

3. The refresher briefing does not have to cover the whole subject of security. As it is unlikely that it will be possible to schedule everyone in the command at the same time, the refresher briefing will probably be more effective if it is tailored for a particular group. For example, the briefing might include some updating on policies and procedures, plus required counter-intelligence reminders, but concentrate on preparation of classified material for clerical personnel or on procedures for classifying and marking

material for those who draft classified documents. A review of the requirements governing handcarrying classified material would be appropriate for those who are most likely to travel on command business or a review of clearance criteria and adjudicative policy would be appropriate for supervisors of cleared personnel.

4. Once every two years, those who have access to Secret or above must be given a counterespionage briefing by a Naval Investigative Service agent. The security manager is responsible for arranging for the briefing with the local NIS office (see appendix D).

3-10 SPECIAL BRIEFINGS

1. Certain types of special briefings are required, to be coordinated by the security manager. These include:

a. Foreign Travel Briefing

(1) Any individual who has had access to classified information who plans to travel to or through a communist controlled country or to attend a meeting, in the United States or elsewhere, in which representatives of communist controlled countries are expected to participate (see exhibit 5A), must be given a defensive briefing. Cruises on Soviet ships, which have become available recently, also require this pre-cautionary briefing. It is recommended that the briefing be coordinated with the Naval Investigative Service.

(2) Audiovisual material for a formal Foreign Travel Briefing is stock-ed at servicing Naval Investigative Service offices (appendix D). Ensure that personnel know that this is a required briefing and that they are responsible for advising the security manager when a situation requiring a "foreign travel" briefing arises.

(3) When the individual returns, he/she should be debriefed to provide the opportunity to report any incident - no matter how insignificant it might have seemed - that could have security implications. A record should be kept of those given the briefing, for follow-up. Check with the Naval Investigative Service office, at the time the audiovisual material is requested, to see if NIS will accomplish the debriefing.

(4) Those who frequently travel, attend meetings or host meetings for foreign visitors need not be briefed at each occasion. Once every six months will suffice.

(5) The foreign travel briefing is only required for those who have had access to classified information but it may be given to dependents, or others without access, if they ask.

5-6 FOREIGN TRAVEL

1. All personnel possessing a security clearance are required to report to their security office all personal foreign travel in advance of the travel being performed. Personnel will be advised of this requirement to report such travel during the orientation briefing and annual refreshers briefings

conducted in accordance with paragraphs 3-7 and 3-9.

2. When travel patterns (i.e., numerous expensive trips abroad or very frequent travel), or the failure to report such travel, indicate the need for investigation, the matter will be referred to the nearest NIS office for action and to the Commander, Naval Security and Investigative Command for information.